3GPP TSG SA #6 **Tdoc TSG SA SP-99585**
Nice, FRANCE
15th - 17th December 1999

Source: TSG SA WG3

Subject: R99 CR to 33.102
Agenda item: 5.3.3

This document contains one CR to 33.102 version 3.2.0 agreed by SA WG3 with the exception of Lucent to be presented to SA#6 for approval.

CR	REV	CAT	SUBJECT	WG_DOC	3G_PHASE
031		C	Removal of alternative authentication mechanism	S3-99542	99

3GPP TSG SA WG 3 (Security) meeting #9 S3-99542
Helsinki, 7—9 December, 1999.

3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102 CR 031 Current Version: 3.2.0

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG SA #6 for approval ☒ for information □ *(only one box should be marked with an X)*
list TSG meeting no. here ↑

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: USIM □ ME □ UTRAN □ Core Network □
(at least one should be marked with an X)

Source:	[TSG SA WG 3]	**Date:**	1999-Dec-09
Subject:	Removal of alternative authentication mechanism described in annex D		
3G Work item:	Security		

Category:
(only one category shall be marked with an X)

F	Correction	□
A	Corresponds to a correction in a 2G specification	□
B	Addition of feature	□
C	Functional modification of feature	□
D	Editorial modification	☒

Reason for change: The alternative authentication mechanism is no longer considered for authentication in UMTS.

Clauses affected: Annex D

Other specs affected:

Other 3G core specifications	□	→ List of CRs:	
Other 2G core specifications	□	→ List of CRs:	
MS test specifications	□	→ List of CRs:	
BSS test specifications	□	→ List of CRs:	
O&M specifications	□	→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

Annex D: Void

~~A mechanism for authentication based on a temporary key~~

~~D.1 Authentication based on a Temporary Key~~

~~D.1.1 General~~

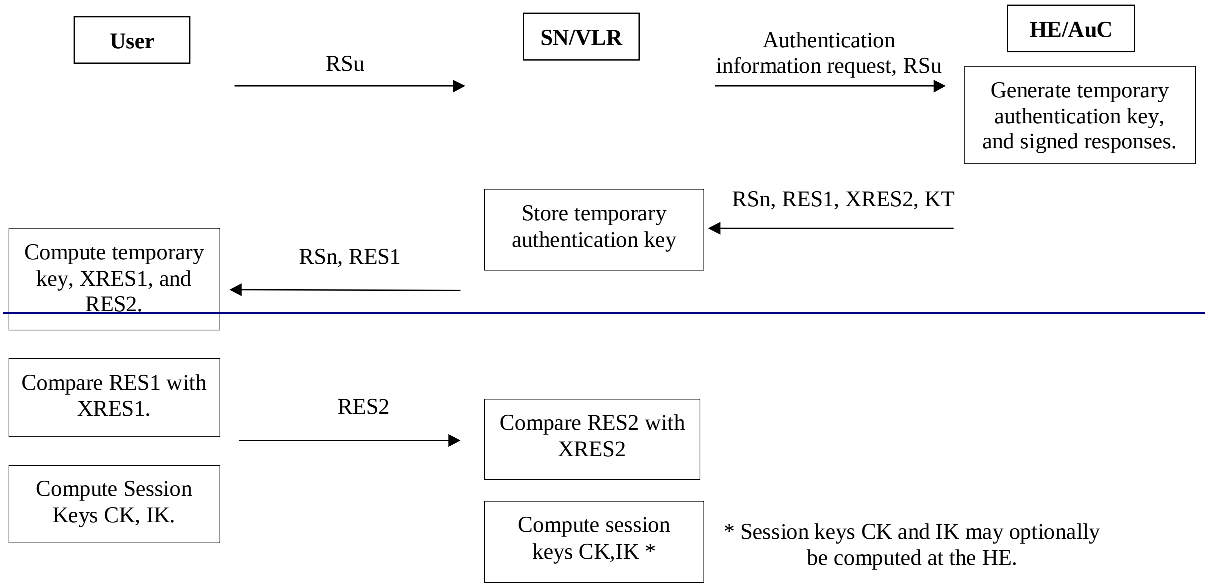
~~The mechanism described here achieves mutual authentication and key agreement between the USIM and the AuC in the user's HE, showing knowledge of a secret key K which is shared between and available only to these two parties. The temporary key generated during the protocol is shared with the visited SN/VLR, and can be used subsequently with the local authentication and session key agreement protocol described in section D.2 or with the other local authentication mechanisms described in section 6.5. Additionally, session keys for the first session are created during the protocol.~~

~~The method was chosen in such a way as to reduce signalling between the HE and the SN/VLR. The method is composed of a mutually authenticated challenge/response protocol with key agreement.~~

~~An overview of the mechanism is shown in Figure D.1.~~

~~When the mobile first requests service from the SN/VLR, a random seed RSu created by the user (USIM or terminal) is included in the request message. The message including RSu is forwarded to the HE/AuC, which generates its own random challenge RSn. An authentication vector is returned to the SN/VLR. The vector contains {RSn, RES1, XRES2, KT}, where RES1 is the response to the user's challenge, XRES2 is the response to the network's challenge which is expected from the user, and KT is the temporary authentication key shared with the SN/VLR. The network's challenge RSn and the network authentication response RES1 are sent to the MS. If the MS verifies RES1, thereby authenticating the identity of the network, it responds with RES2 and generates the new temporary key KT. The SN/VLR then verifies that RES2 equals XRES2, thereby authenticating the identity of the USIM, and stores the new temporary key KT. Furthermore, both the USIM and the SN/VLR immediately use KT with the random seeds RSu and RSn to generate the first session keys CK and IK. The established keys CK and IK will then be transferred by the USIM and the SN/VLR to the entities which perform ciphering and integrity functions.~~

~~The SN/VLR can offer secure service to the USIM without reference to the home system HE/AuC by using the temporary key KT. This local authentication mechanism is described in section D.2.~~


User
SN/VLR
HE/AuC
RSu
Authentication information request, RSu
Generate temporary authentication key, and signed responses.
RSn, RES1, XRES2, KT
Store temporary authentication key
RSn, RES1
Compute temporary key, XRES1, and RES2.
Compare RES1 with XRES1.
RES2
Compare RES2 with XRES2
Compute Session Keys CK, IK.
Compute session keys CK,IK *
* Session keys CK and IK may optionally be computed at the HE.

~~**Figure D.1: Authentication**~~

~~The authenticating parties shall be the AuC of the user's HE (HE/AuC) and the USIM in the user's mobile station. The mechanism consists of the following procedures:~~

~~A procedure to generate a new temporary authentication key and session keys, and distribute the temporary authentication key from the HE/AuC to the SN/VLR. This procedure is described in D.1.2. The SN/VLR is assumed to be trusted by the user's HE to handle authentication information securely. It is also assumed that the intra-system links between the SN/VLR to the HE/AuC are adequately secure. Mechanisms to secure these links are described in clause 7. It is further assumed that the user trusts the HE.~~

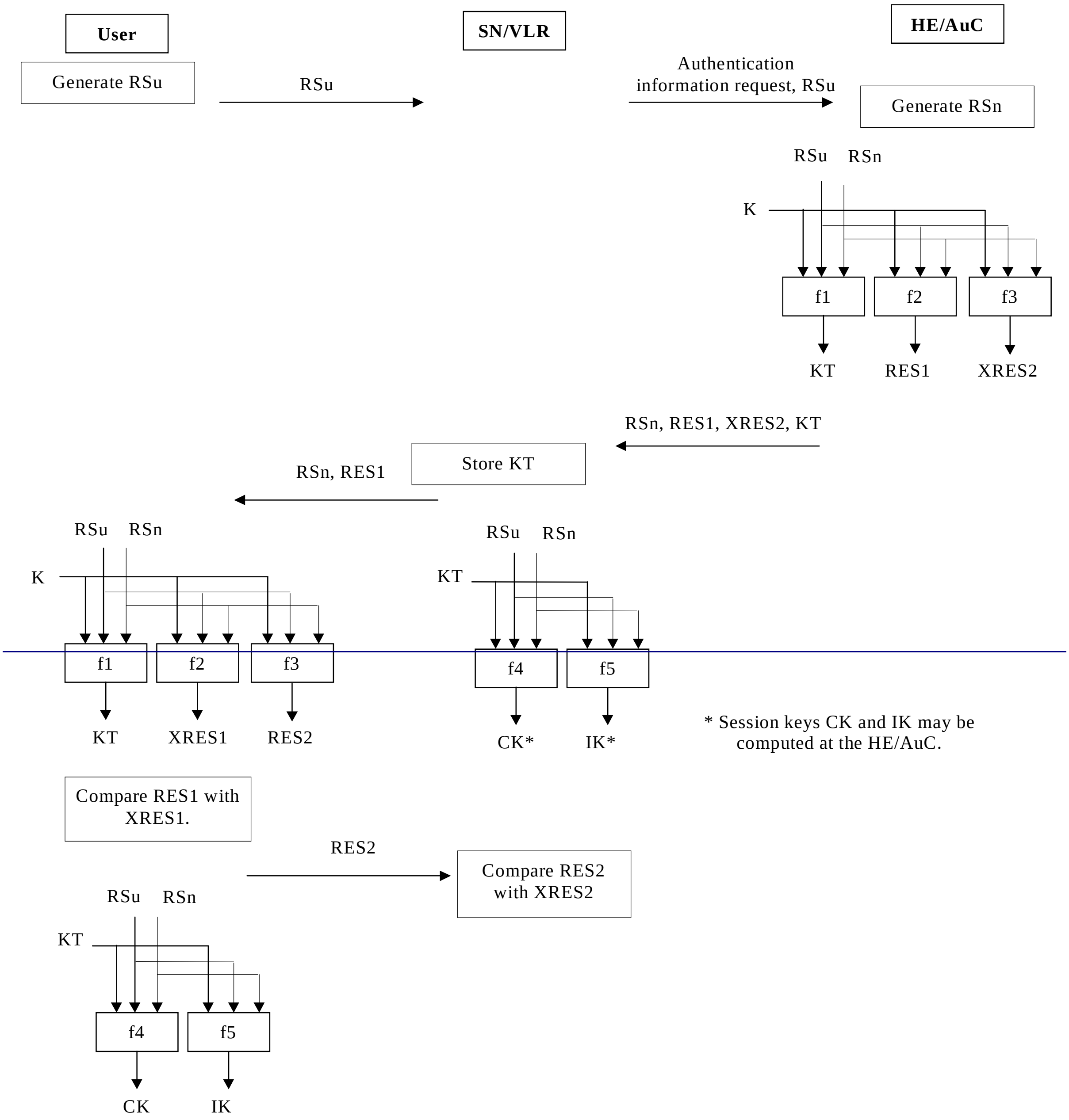
~~A procedure to distribute the temporary authentication key from a previously visited VLR to the newly visited VLR. This procedure is described in D.1.3. It is also assumed that the links between SN/VLRs are adequately secure. Mechanisms to secure these links are described in clause 7.~~

~~D.1.2 Temporary Key Generation with Session Key Agreement~~

~~The services provided by this mutually authenticated key agreement protocol are:~~

- ~~the SN/VLR authenticates the MS;~~
- ~~the MS verifies that the SN/VLR is allowed to offer it services on behalf of its HE;~~
- ~~the MS and the HE establish a new temporary authentication key with freshness guarantees to both parties;~~
- ~~the HE distributes this temporary key to the SN/VLR for subsequent use in local authentication protocols; and,~~
- ~~the MS and the SN/VLR establish new cipher and integrity keys with freshness guarantees to both parties.~~

~~The procedure is illustrated in Figure D.2.~~



~~**Figure D.2: Temporary Key Generation Protocol**~~

~~The user (USIM/terminal) invokes the procedure by requesting service from the SN/VLR. This service request contains an unpredictable random seed RSu, generated by the user. The SN/VLR sends the HE/AuC an *authentication data request*, which includes RSu as well as either the IMUI or an EMUI for the user. In case an EMUI is used, the mechanism described in 6.2 is integrated in this procedure.~~

~~Upon the receipt of the authentication data request from the SN/VLR, the HE/AuC generates the authentication vector. To generate an authentication vector AV the HE/AuC generates an unpredictable random value RSn. Subsequently the following values are computed:~~

- ~~a temporary key KT = $f1_K$(PAR1 || RSu || RSn) where f1 is a key generating function.~~
- ~~an authentication response RES1 = $f2_K$ (PAR2 || RSu || RSn) where f2 is a (possibly truncated) MAC function.~~
- ~~an expected response XRES2 = $f3_K$ (PAR3 || RSu || RSn) where f3 is a (possibly truncated) MAC function.~~

~~Note 1: The need for f2 and f3 to use a long-term key different from K is ffs.~~

~~Note 2: It is also ffs in how far the functions f1, ..., f5 need to differ and how they may be suitably combined.~~

~~Note 3: PAR1, ..., PAR5 are different fixed initial values which may be used when similar or identical functions are used for f1, ..., f5. The need for the inclusion of PAR1, ... PAR5 is ffs. When omitted they may be thought of as being integrated in the definition of the functions f1, ..., f5 respectively.~~

~~These authentication parameters are used to construct an ordered array of authentication vectors for the user consisting of {RSn, RES1, XRES2, KT}.~~

~~The HE/AuC sends the requested authentication vector to the SN/VLR in a response message.~~

~~The serving system SN/VLR may generate the session keys locally, or they may be generated by the HE/AuC and sent to the SN/VLR. In either case, the following session keys are computed:~~

- ~~a cipher key CK = $f4_{KT}$ (PAR4 || RSu || RSn) where f4 is a key generating function.~~
- ~~an integrity key IK = $f5_{KT}$ (PAR5 || RSu || RSn) where f5 is a key generating function.~~

~~Note 4: The requirements on f4 and f5 are ffs.~~

~~Note 5: (See notes 2 and 3 above).~~

~~The SN/VLR sends to the user the random challenge RSn and the network's authentication response RES1, taken from the authentication vector.~~

~~Upon receipt of RSn and RES1 the user first computes XRES1 = $f2_K$ (PAR2 || RSu || RSn) from RSu, RSn, and the secret key K, and compares this with the value of RES1 received from the SN/VLR. If they are unequal, the user sends a message back indicating that the authentication token was corrupt and abandons the authentication protocol. If the equality holds, the user has authenticated the identity of the home system.~~

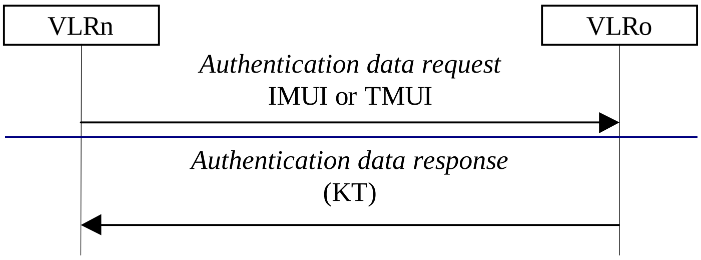
~~The user then computes RES2 = $f3_K$ (PAR3 || RSu || RSn), which is sent back to the SN/VLR, and the temporary key KT = $f1_K$ (PAR1 || RSu || RSn). KT is subsequently used to generate the cipher key CK = $f4_{KT}$ (PAR4 || RSu || RSn) and the integrity key IK = $f5_{KT}$ (PAR5 || RSu || RSn). Note that if this is more efficient, XRES1, RES2, KT, CK and IK can be computed earlier at any time after receiving RSn (although KT must be computed before CK and IK).~~

~~When the SN/VLR receives RES2 it compares it with the expected response XRES2 from the selected authentication vector. If XRES2 equals RES2 then the user is authenticated. The SN/VLR also distributes the derived cipher key CK and derived integrity key IK to the appropriate entities for integrity and ciphering.~~

~~D.1.3 Distribution of temporary keys between VLRs~~

~~The purpose of this procedure is to provide a newly visited VLR with the current temporary authentication key from a previously visited VLR.~~

~~The procedure is initiated by the visited VLR and illustrated in the following figure:~~



~~Figure D.3: Distribution of authentication data between VLRs~~

~~The procedure is invoked by the newly visited VLRn after a location update request of the user. Typically the user identifies himself using a temporary user identity TMUIo and the location area identity LAIo of a location area under the jurisdiction of VLRo. In that case this procedure is integrated with the procedure described in 6.1.~~

~~Upon receipt of the request the VLRo verifies whether it has a current temporary authentication key in its database and if so, sends the current temporary authentication key to VLRn. The previously visited VLRo deletes the temporary authentication key from its database.~~

~~Upon receipt the VLRn stores the temporary authentication key. If VLRo indicates that it has no current temporary authentication key or the VLRo cannot be contacted, VLRn should request new a authentication vector from the user's HE using the procedure described in D.1.2.~~

~~D.1.4 Handover~~

~~[More detailed description on handover from GSM to a TETRA-based network, and vice-versa, is ffs]~~

~~In case of handover the security level of the network entered by the user has to be fulfilled.~~

~~Therefore the following functionality has to be provided in case of handover:~~

~~Re-authentication using the (probably network specific) authentication mechanisms of the system entered by the user in case of handover.~~

~~Note: There is only one exception, when UMTS operators allow a user to roam in their networks with a GSM subscription.~~

~~Note: In case of inter-system/intra-operator handover (between GSM and UMTS) there is no strong requirement for re-authentication because of the original authentication having been done by the same operator, because of the service capabilities after handing over will be equivalent to GSM level. After service termination re-authentication and LUP has to be fulfilled as required for roamers.~~

~~This is restricted to phase 1. In future releases of phase 1 and later phases, mechanisms shall be specified to enable the level of security, after an inter-system or inter-operator handover, which normally is achieved in the radio network to which handover is done.~~

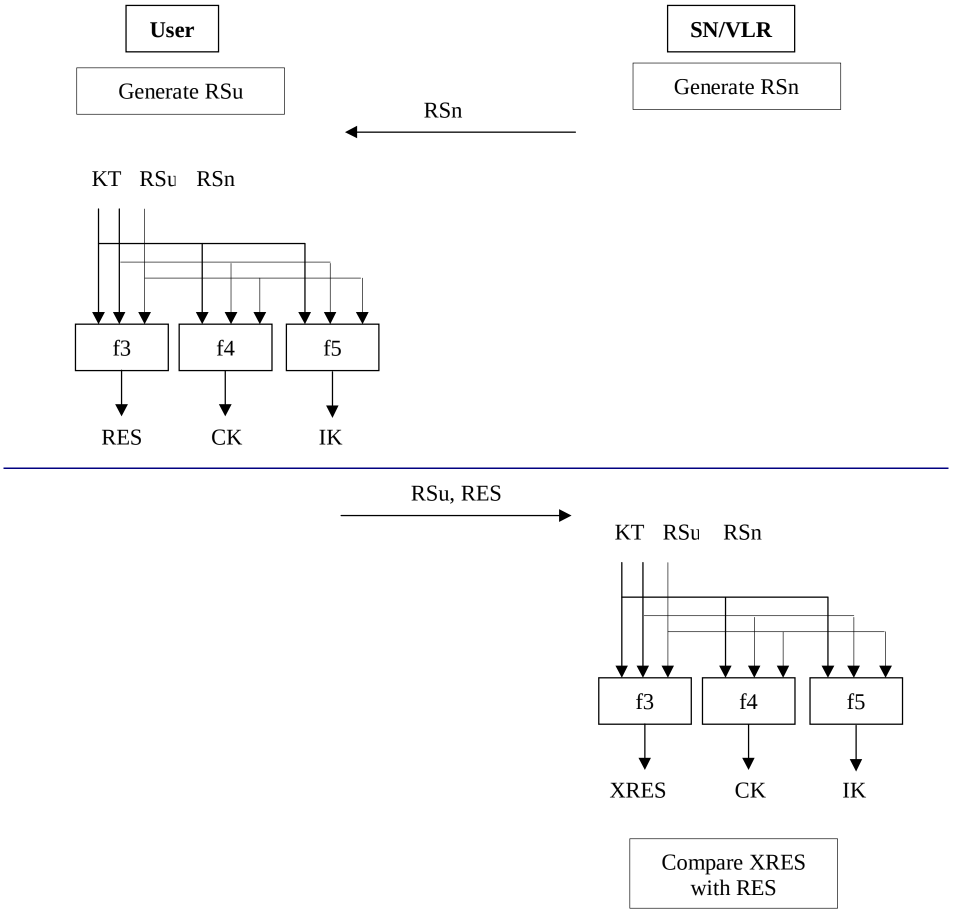
~~D.2 Local authentication~~

~~D.2.1 Session Key Agreement based on Temporary Authentication Key~~

~~The services provided by this mutually authenticated key agreement protocol are:~~

- ~~the SN/VLR authenticates the MS;~~
- ~~the MS verifies that the SN/VLR is allowed to offer it services on behalf of its HE;~~
- ~~the MS and the SN/VLR establish new cipher and integrity keys with freshness guarantees to both parties.~~

~~The procedure is illustrated in figure D.4.~~



~~**Figure D.4: Locally authenticated session key agreement**~~

~~The SN/VLR initiates the procedure. It generates a unpredictable random challenge RSn which is sent to the user.~~

~~The user (USIM/terminal) generates its own random challenge RSu. Upon receipt of the network's challenge RSn, the user calculates the following values:~~

- ~~an authentication response RES = $f3_{KT}$ (PAR3 || RSu || RSn) where f3 is a (possibly truncated) MAC function.~~
- ~~a cipher key CK = $f4_{KT}$ (PAR4 || RSu || RSn) where f4 is a key generating function.~~
- ~~an integrity key IK = $f5_{KT}$ (PAR5 || RSu || RSn) where f5 is a key generating function.~~

~~Note 1: (See notes 1-5 in Clause D.1.2)~~

~~The USIM/terminal sends the network the random challenge RSu and the authentication response RES, and distributes the session keys CK and IK to the appropriate entities for ciphering and integrity.~~

~~Upon receipt of RSu and RES the SN/VLR computes XRES = $f3_{KT}$ (PAR3 || RSu || RSn) from RSu, RSn, and the temporary authentication key KT that is stored in the VLR database, and compares this with the value of RES received from the user. If they are unequal, the network sends a message back indicating that authentication has failed and abandons the authentication protocol. If the equality holds, the user is authenticated to the network.~~

~~The SN/VLR then computes the ciphering key CK = $f4_{KT}$ (PAR4 || RSu || RSn) and the integrity key IK = $f5_{KT}$ (PAR5 || RSu || RSn), which it distributes to the appropriate entities for ciphering and integrity.~~

~~D.3Criteria for replacing the authentication “working assumption”~~

~~One of the following conditions should be met before considering replacement of the authentication “working assumption”:~~

- ~~A serious security flaw is discovered with the SQN protocol. A “serious flaw” is a weakness that allows a demonstrable attack on the authentication system, leading to theft of service (fraud), compromise of privacy, or any degradation below the security level of current systems. If the flaw can be easily fixed without changing the fundamental nature of the protocol, there are no grounds for replacement.~~

- ~~Serious operational difficulties are discovered with the SQN protocol. These are problems implementing the protocol that may be discovered during early development or testing. A “serious operation difficulty” is one that prevents the successful and reliable completion of the protocol. If the problem can be solved with a simple alteration that does not change the fundamental nature of the protocol, there are no grounds for replacement.~~